Department of Energy
Washington, DC 20585

January 15, 2025

DOE’s Implementation of M-24-15: Modernizing the Federal Risk and Authorization Management Program (FedRAMP)

TO: Office of the Federal Chief Information Officer,
Office of Management and Budget

FROM: Ann Dunkin,
Chief Information Officer
Department of Energy

SUBJECT: Department of Energy’s Agency-Wide Policy for Modernizing the Federal Risk and Authorization Management Program (FedRAMP)

Congress enacted the FedRAMP Authorization Act in December 2022 which established the Federal Risk and Authorization Management Program (FedRAMP) to provide “a standardized, reusable approach to security assessment and authorization for cloud computing products and services that process unclassified information used by agencies.”[1] On July 25, 2024, OMB issued OMB Memorandum M-24-15, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)*, which defines the scope of FedRAMP and establishes related requirements for agencies.[2] Within 180 days of the issuance of that memorandum—by January 21, 2025—each agency is required to issue or update agency-wide policy that aligns with the memorandum’s requirements. By that same date, each agency must also submit to OMB “all agency policies relating to the authorization of cloud computing products and services.”[3]

- **DOE Response:** Department of Energy (DOE) Order 205.1D, *DOE Cybersecurity Program*, issued in April 2024, serves as the Department’s official policy directive for implementing cybersecurity laws, executive orders, regulations, and policies. DOE O 205.1D requires departmental offices and programs to “abide by the FedRAMP Authorization Act per H.R. 7776, National Defense Authorization Act for Fiscal Year 2023, and subsequent OMB guidance applicable to the Act, and the DOE FedRAMP Agency Authorization Process.” The process of revising DOE orders occurs through the Department’s Directives Review Board, and an update to DOE O

[1] 44 U.S.C. §§ 3608-16
[2] Available at https://www.whitehouse.gov/wp-content/uploads/2024/07/M-24-15-Modernizing-the-Federal-Risk-and-Authorization-Management-Program.pdf
[3] 44 U.S.C. § 3613(d).

205.1 is scheduled to kick-off later in FY2025. In the interim, the DOE Office of the Chief Information Officer (OCIO) is using amplification guidance, along with the Department's existing FedRAMP authorization process guide, to support the Department in implementation of the additional requirements of M-24-15 until DOE formally updates departmental policy through DOE O 205.1E. The Department's agency-wide FEDRAMP guidance consists of DOE O 205.1D, the DOE OCIO's FedRAMP amplification guidance, and the DOE OCIO FedRAMP Agency Authorization Process Guide.

******

Scope: Section III M-24-15 requires agencies to obtain and maintain a FedRAMP authorization for cloud computing services that create, collect, process, store, or maintain unclassified Federal information on behalf of a Federal agency and are not among the excepted categories of services described by the memorandum.

Policy Submission:

- Please identify and attach a copy of your agency's policy or policies addressing when a cloud product or service must be FedRAMP-authorized. If your agency does not have a formal policy addressing the subject, please describe any informal policy that may guide agency practice. If your agency has neither a formal nor an informal policy on this subject, please explain how your agency ensures compliance with M-24-15 and the FedRAMP Authorization Act.

- **DOE Response:** DOE Order 205.1D, *DOE Cybersecurity Program*,[4] serves as the Department's official policy directive for implementing cybersecurity laws, executive orders, regulations, and policies. DOE O 205.1D requires Departmental offices and programs to "abide by the FedRAMP Authorization Act per H.R. 7776, National Defense Authorization Act for Fiscal Year 2023, and subsequent OMB guidance applicable to the Act, and the DOE FedRAMP Agency Authorization Process." The *DOE FedRAMP Agency Authorization Process Guide*[5] implements the DOE O 205.1D FedRAMP standards, enforcing that, "All cloud services used by DOE organizations are required to have a FedRAMP Authorization to Operate (ATO)." The Department is currently working to update its internal processes to address the enhanced authorization requirements of M-24-15 by the end of Q4 FY2025 (September 2025).

[4] Department of Energy Cybersecurity Program

[5] DOE-FedRAMP-Agency-Authorization-Process-Guide_v1.2_Signed

Obtaining FedRAMP Authorizations: The FedRAMP Authorization Act requires OMB "to issue guidance that includes requirements for agencies to obtain a FedRAMP authorization when operating a cloud computing product or service" that is within the scope of FedRAMP.[6] Pursuant to that statutory requirement, Section III of M-24-15 states "agencies must obtain and maintain a FedRAMP authorization when the cloud product or service falls within the scope of this section." Therefore, if an agency seeks to use an in-scope cloud product or service that does not have a FedRAMP authorization, the agency must work with FedRAMP to obtain a FedRAMP authorization for that cloud product or service consistent with the FedRAMP Authorization Process outlined in Section IV of M-24-15.

Policy Submission:

- Please identify and attach a copy of your agency's policy or policies requiring a FedRAMP authorization for cloud services or products that are within the scope of the program, and describing the process for complying with that requirement. If your agency does not have a formal policy addressing the subject, please describe any informal policy that may guide agency practice. If your agency has neither a formal nor an informal policy on this subject, please explain how your agency ensures that any in-scope cloud products or services it uses are FedRAMP-authorized.

- **DOE Response:** DOE established a FedRAMP authorization process in 2020 and issued an internal process guide, the *DOE FedRAMP Agency Authorization Process Guide*, for implementing DOE's FedRAMP authorization program. The DOE OCIO serves as the FedRAMP sponsoring organization for any cloud computing product or service that DOE seeks to acquire. Under DOE policy, any DOE organization may request and/or recommend a FedRAMP Agency ATO. The DOE OCIO is working with programs offices and sites to identify cloud systems in use at the Department that are non-compliant with FedRAMP authorization requirements. Any use of non-FedRAMP approved products is a variance from departmental policy and must have a documented justification and approval for use by the designated authorizing official (AO). At a minimum, non-compliant cloud products must demonstrate their compliance with one of the FedRAMP security baselines in accordance with the FedRAMP Authorization Act.

Leveraging FedRAMP Authorizations: Section VII d.4 requires agencies to leverage other agency security authorization materials within the FedRAMP repository to the greatest extent possible.

[6] 44 U.S.C. § 3615

Policy Submission:

- Please identify and attach a copy of your agency's policy or policies regarding use of existing FedRAMP materials for the authorization of in-scope cloud services or products. This should include any policy explaining how agency personnel should access FedRAMP authorization materials. If your agency does not have a formal policy addressing these issues, please describe any informal policy that may guide agency practice. If your agency has neither a formal nor an informal policy addressing these issues, please explain how your agency ensures that it relies upon existing FedRAMP authorization materials to the greatest extent possible. For example, your agency might maintain a catalog listing products and services that have already been authorized at your agency or that have a FedRAMP authorization.

- **DOE Response:** The *DOE FedRAMP Authorization Process Guide* outlines the steps for DOE personnel to access FedRAMP authorization materials upon request. The DOE OCIO maintains an internal list of FedRAMP authorized systems; in response to M-24-15, DOE OCIO is considering options for making this list available to the larger DOE enterprise by the end of Q1 FY2026 (December 2025).

Presumption of Adequacy: The FedRAMP Authorization Act states that "the assessment of security controls and materials within the authorization package for a FedRAMP authorization shall be presumed adequate for use in an agency authorization to operate cloud computing products and services."[7] Accordingly, if a given cloud product or service has a FedRAMP authorization at a given FIPS 199 impact level, agencies must presume the security assessment documented in the authorization package is adequate for their use in issuing an authorization to operate at or below the FIPS 199 impact level.[8] It is important to note that the presumption of the adequacy of a FedRAMP authorization does not supersede or modify the authorities and responsibilities of agency heads under FISMA.

Policy Submission:

- Please identify and attach a copy of your agency's policy or polices implementing the presumption of adequacy. If your agency does not have a formal policy implementing the presumption, please describe any informal policy that may guide agency practice. If your agency has neither a formal nor an informal policy on the presumption, please explain how your agency ensures that it treats the security controls and materials within an existing FedRAMP authorization as presumptively adequate for the agency's use.

[7] 44 U.S.C. § 3613(e)(1).

[8] M-24-15 at 6.

- **DOE Response:** DOE processes support the use of a presumption of FIPS 199 security categorization adequacy in the re-use of security assessment document at the approved security categorization impact level. In response to M-24-15, DOE OCIO will review and update its *DOE FedRAMP Agency Authorization Process Guide* to provide additional information to Departmental Elements (DEs) and cloud service providers (CSPs).

Additional Requirements When Reusing a FedRAMP Authorization: Once an agency issues an authorization to operate or use based on a FedRAMP authorization, the agency is required pursuant to M-24-15 to provide to the FedRAMP PMO a copy of the authorization letter and any relevant supplementary information, including agency-specific configuration information, as deemed appropriate, that may be helpful to other agencies upon issuance of an authorization to operate or use based on a FedRAMP authorization. Additionally, agencies must ensure all artifacts meet FedRAMP requirements and are sufficient for reuse by other agencies. Finally, agencies must ensure all authorization materials provided to the FedRAMP PMO are in machine-readable and interoperable formats in accordance with any applicable guidance from FedRAMP.

Policy Submission:

- Please identify and provide a copy of any agency policy or policies intended to ensure that the required materials are transmitted to FedRAMP in the required formats and are sufficient for reuse by other agencies. If your agency does not have a formal policy meeting that description, please describe any informal policy that may serve the same purpose. If your agency has neither a formal nor an informal policy, please explain how your agency ensures that the required materials are transmitted to FedRAMP in the required formats and are sufficient for reuse by other agencies.

- **DOE Response:** DOE OCIO directs CSPs to develop security assessment documentation in interoperable and machine-readable formats. Currently, the Department does not mandate a specific format or machine-readable language for its ATO documentation. The DOE OCIO, including the Department's Chief Data Officer, is assessing available formatting standards for Departmental data products. Once these formatting standards are defined, DOE OCIO will direct CSPs to use these standards for submitted documentation.

Continuous Monitoring: M-24-15 requires agencies to continuously diagnose and mitigate against cyber threats and vulnerabilities associated with usage of cloud service offerings. Additionally, agencies are required to regularly review continuous monitoring materials provided by CSPs.

Policy Submission:

- Please identify and provide a copy of any agency policy or policies regarding the review of continuous monitoring materials provided by CSPs. If your agency does not have a formal policy meeting that description, please describe any informal policy that may serve the same purpose. If your agency has neither a formal nor an informal policy, please explain how your agency will regularly review continuous monitoring materials.

- **DOE Response:** DOE OCIO has a robust continuous monitoring (ConMon) process in place for FedRAMP approved systems. The *DOE FEDRAMP Agency Authorization Process Guide* outlines the steps and required activities of DOE's ConMon process. In addition, the DOE OCIO utilizes the USDA Connect dashboard to evaluate and share CSP vulnerabilities. On average, DOE OCIO conducts one CSP continuous monitoring review per month. The DOE OCIO ConMon team works with other cybersecurity programs within the DOE OCIO to share information on identified cyber threats and vulnerabilities.